Journal of Theoretical and Applied Information Technology
10th August 2013. Vol. 54 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MEMORABILITY FEATURES OF DRAW-BASED GRAPHICAL PASSWORDS

[1]OBASAN ADEBOLA O., [2]NORAFIDA ITHNIN, [3]CHUA SIEW WENG
[1,2&3] Universiti Teknologi Malaysia, Faculty of Computing,
81310 UTM, Skudai, Jorhor-Bahru, Malaysia
E-mail: [1]aolukay@yahoo.com, [2]afida@utm.my, [3]csiewweng@hotmail.com

Corresponding Author: Obasan Adebola O. Department of computer systems & Communnication, IASRG Lab, Faculty of Computing at University Technology Malaysia, 81310, Skudai ,Johor Bahru, Malaysia

ABSTRACT

Password authentication has become a widely recognized element of computer security practices, where human users are proven or confirmed as legitimate users for access to secure systems. Every user needs to recall its password correctly before access can be granted to an intended system. Remembering the secure password chosen from mixture of random alphanumeric and non-alphanumeric characters is an everyday problem for all users because of individual memory limitation. In an effort to solve this problem, users tend to choose insecure passwords that are making most systems vulnerable to many attacks. Instead of using secure-but-difficult to remember or unsecure-but-easy to remember alphanumeric password, now graphical password which works just by clicking with a mouse or stylus could be used for user authentication. Graphical password is able to solve the problem of alphanumeric password being hard to remember. The main objective of this paper is to provide a comprehensive survey of array of draw-based graphical password schemes and capture the memorability of each scheme in a table. We highlight what makes images memorable and recommend that choice of background image in a scheme could affect how memorable it is because not all images are equal in memory.

Key words: Graphical passwords, Password space, Authentication, images memorability

1. INTRODUCTION

In modern days applications, Information systems are taking over all our day-to-day activities being banking, accounting, and others , as such they require some measures of control and protection to ensure reliability , integrity , and other security goals. In order to achieve reasonable level of protection , username-password methods have been widely used as method of choice for identifying, authenticating, and authorizing users by many banks ,government , and corporate bodies and even all websites on the internet. An average internet user manages not just one but multiple accounts that require use of passwords [1]. The user identification is employed to identify a user to the system while the authentication proves user's claimed identity as being right or wrong depending on username and corresponding password . In order to complete used authentication process, authorization deals with the users' right to access resources ones they are authenticated. Text-based password method was introduced in the 1960s as a security measure to restrict access of useful information to authorized users within a computer system setup or worldwide networked computers .

However, it is popularly known that text passwords are vulnerable and insecure for a number of security flaws. The main problem of text passwords as user means of authentication is that users find it difficult to remember secure passwords which are expected to be random or meaningless strings of different characters: lower and upper case letters (a-z and A-Z), digits (0-9) and special symbols (#,&,..). Intensive studies in this area have revealed that users tend to pick short passwords or passwords that are meaningful or not difficult to remember [1]. Unfortunately, such meaningful strings are weak text passwords which can be easily guessed or broken by an attacker who strives maliciously to obtain the legitimate user passwords. In the year 1990, a comprehensive study was carried out by Klin, where it was discovered that about 25% of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

valid passwords of the scheme were successfully found from a list of all the likely 3 x 10^6 passwords made to carry out an attack on 2 x 10^{14} 8-character passwords made up of mixture of lower and upper case letters and digits. Also, the credential information such as usernames, passwords, and credit card details text passwords can be captured or stolen by malicious software. Such an attack occurs due to the fact that text passwords do not allow mutual authentication between users and server. By design, passwords are made to provide only user authentication, and does not allow server authentication by the user. So a malicious server can present itself as the legitimate one. This means that text password systems are characterized by many inadequacies which could necessitate other systems such as symmetric and public cryptography technology to derive safe and extremely long cryptographic key from a weak or memorable user-chosen password with the help of some strong authentication protocols such as Encrypted Key Exchange and Password Authentication Key Exchange to produce a more secure password for network communications. Other alternative technologies include security token, biometric, cognitive passwords and even hybrid of these authentication factors are gaining much attention to overcome problems in the text-based password authentication. However, the problem with these systems is that most of them are designed by the service providers to be cost effective , scalable and secure , which sometimes creates difficulty and poor usability or memorability from the users' perspective. As a result if these limitations and others, graphical passwords lime light to provide better systemic usability and memorability.

2. RELATED WORK

The major weak spot of text-based passwords of knowledge-based authentication is caused by the fact that this system of authentication requires human memory task called pure recall which is weaker than other alternatives which are cued recall memory and recognition memory [2]. In studies titled *picture superiority effect* revealed that human brains function better in recalling or recognizing images than texts or words. Meaning that recall process of human memory could be enhanced by using images or pictures as a means of authentication rather than string of texts. Based on this notion the idea of graphical passwords for authentication was formed.

The first graphical password alternative was implemented in 1996 by Greg Blonder , based on premise that humans memory has the capacity to retains visual information longer than words or texts. Graphical password schemes also emerged and highly suitable to provide access to systems that are not keyboard-based as a means of data input. Examples of such systems include ATMs, PDAs, PCs to mansion a few. In our day-day applications, they all use some form of input device that allow pointing, selecting, clicking , drawing or other graphical-based functions. Examples, stylus in PDAs mouse on PCs and touch screens at ATMs.

2.1 Types of graphical passwords

Generally, graphical password systems require use of visual information to identify a user by selecting a number of images , or by drawing a shape as a means of authentication. To be authenticated, the users are later asked to recall the selected images or redraw the drawn shape. The user authentication is successful if the user is able to provide a match. In literature, the existing graphical passwords are grouped in different classifications, based on a number of factors like the following:

- Based on cognitive activities or memory task of the user required to remember and enter the password. By this classification, we have recall-based , cue recall-based and recognition-based schemes [3] .

- Based on types of background used for the password schemes. By this classification, we have graphical passwords divided into Image-based and grid-based schemes [4].

- Based on how the required graphical device such as mouse, stylus is to be used in the password scheme. By this classification, we have graphical passwords into three types, namely; draw-based, click-based and choice-based schemes [5] .

However, all these classifications mean the same thing in different ways depending on reader's understanding on each of them. For the purpose of this survey , we consider classification based on how the required graphical devices are use in the schemes. In draw-based

Journal of Theoretical and Applied Information Technology
10th August 2013. Vol. 54 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

schemes , users use the graphical devices like mouse or stylus to draw their passwords and reproduce the secret drawings in order to be authenticated. Examples of these schemes include DAS, BDAS, Qualitative DAS, Grid Selection , Multi-Grid DAS, Pass-Go, and Passdoodle. In click-based schemes of this classification, the user is expected to make a number click points depending on the system settings in a specific order. While in choice-based schemes, the user is challenged with authentication rounds, depending on number of images chosen and to be remembered, each round involves multiple images. Good number of these schemes will be studied in this paper.

2.2. Draw-based graphical password systems

In a draw-based graphical system also called drawmetric systems, user typically draws and reproduces their password on a 2D grid to verify its identity. The coordinates of the drawing are stored for authentication where user is asked to recall and enter the drawing in the order of the drawing instead of alphabets as it were in text-based passwords . This approach is alphabet independent and as such making it equally accessible for users of any language . The many idea behind this form of password schemes was to develop a graphical authentication system that could be used on small-sized device like PDAs and smart phones that require authentication in a confined environment, where malicious people cannot spy the secret drawing easily [6] . These systems exist in different forms, they include DAS, BDAS etc.

2.2.1 Drawing-A – Secret

Draw-A-Secret (DAS) , is a the first of its kinds. This form of graphical password and was proposed by Jermyn et al. in the year 1999 and motivated primarily by PDAs that offer graphical input capabilities. DAS is a purely graphical password selection and input scheme. The scheme replaces in part password strings, with a picture drawn on a 2D, that is (5 x 5) grid using a stylus or mouse as in the following figure 1. Instead of typing a password, DAS authentication method allows users just to reproduce the drawing process to login. This process must take into account the shape, the start and end points, and the directionality, are limited to tapping and tracing a line or a circle for improving the slow speed of sign-ins by using this method. Suppose that the user is given a stylus with which she can draw a design on this grid. Usually, the drawing consist of one single continuous stroke or multiple strokes separated by " pen-ups" like (6,6), (7,7) or any other coordinated outside the limit, in case in 5x5 grid system. In DAS system, the password is encoded as a set of the coordinates of the cells along the path of the drawing on the grid. Therefore, the length of the password is given by the number of cells the drawing has with a distinguished coordinate pair inserted in the sequence for each ``pen up'' event, i.e., whenever the user lifts the stylus from the drawing surface as illustrated in figure 1. The encoded DAS passwords are stored by the system to be used for the purpose of authentication. In order not to store them in plaintexts, an encryption/decryption key is derived from a DAS password by using cryptographic hash function like SHA-1. Again, for authentication , users are asked to recall the picture in the coordinate sequence . Correct coordinate sequence authenticates the user while wrong coordinate sequence (gestures) will always deny a login, and it will lock out the system after five unsuccessful attempts, until a text password is provided [7]. Jermyn et al. proved that doodles are harder to crack due to a theoretically much larger number of possible doodle passwords than text passwords.

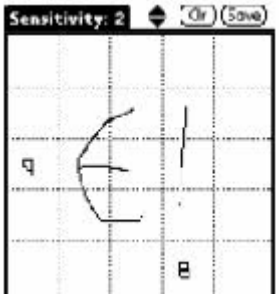

Figure 1: Draw-A-Secret (DAS) (Jermyn, Mayer et. al.

Up- to- date studies reveal that , there is little or no definite information on either the usability or security of the original DAS recall-based system because it has only been user tested through paper prototypes. This makes it difficult to get very accurate and reliable usability or security analysis of DAS system.

Several studies were conducted on DAS to analyze the memorable password space . In 2002 , a user study using "paper prototype" of the system was conducted by J. Goldberg et al. to explore the use of a hand-drawn doodle password ("passdoodle") [8]. The findings of their study show that users could recall all visual

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

elements of the doodle as well as they could recall alphanumeric passwords, but most could not perfectly redraw their selected doodles. Users perceive passdoodles as easier to remember than alphanumeric passwords; however, they prefer whichever authentication method they perceive to be more secure. Also, the results of the study could be used to serve as guidelines for future prototype development.

In 2004, another user study was conducted by Nali and Thorpe on DAS-like scheme where 16 participants were used to draw "doodles " and "logos" 6 each on 6 x 6 grids . The objective of this study is to focus on usability challenge with the DAS scheme and to establish whether or not user drawings contain the predictable characteristics relating:

- to symmetry drawings, number of composite strokes, and
- centering within the grid.

It was found in their result that users drawings contain the predictable characteristics relating to symmetry with few pen strokes, and users tend to draw within the center of the grid. In other words, this means that DAS users tend to choose weak passwords, and their choices would alternately render the scheme less secure in real life.

2.2.2 Background Draw A Secret Graphical Passwords (BDAS)

This is a scheme designed with the primary aim of improving the limitations of DAS scheme in terms of large password space and memorability ,an image background was made by Paul Dunphy and Jeff Yan to come up with BDAS [9]. BDAS scheme is exactly the same as DAS except that image background was superimposed over the blank canvas DAS grid to help users remember where they began the drawing that is being used as a password as illustrated in figure 2. In this way it was showed that people aided with background images tend:

- To set significantly more complicated passwords than their counterparts using the DAS scheme.
- To reduce predictable characteristics in DAS passwords such as symmetric and centering within the drawing grid.
- To improve the strength of the passwords.
- DAS scheme with a background image enhances memorability of the more complex and secure passwords.

Therefore, BDAS with a simple enhancement turns out to be a more effective system than DAS for user authentication in terms of enhanced usability and security of graphical passwords.

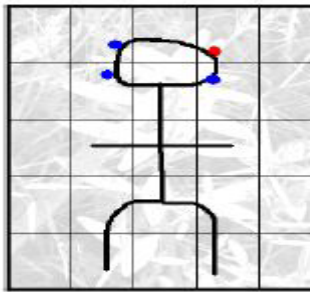

Figure 2: BDAS Graphical scheme

2.2.3 Grid Selection

In 2004, a remarkable research study was proposed by Thorpe and Van Oorschot to improve the DAS security. The method called Grid Selection with zoom feature which enable the user to select a drawing grid. In this technique, a large scale grid (e.g. 35×35) is offered and a user is required to choose a small drawing grid and then draw the password as illustrated in figure 3. They had aim of strengthening security and increasing the size of password space of DAS technique [10]. The grid selection technique enables the users to select a drawing grid in which to draw their passwords. The result of their study showed that the item which has the greatest effect on the DAS password space is the number of coordinate pairs otherwise known as strokes. By implication , this means that for a fixed password length, if a few strokes are chosen then the password space will appreciably reduce [10]. The two main limitations are as follows:

- input a password can be a challenge if a user has problem in identifying the correct grid cell used.

Journal of Theoretical and Applied Information Technology
10th August 2013. Vol. 54 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- it so predictable that most of users will still choose symmetric passwords when using this method.

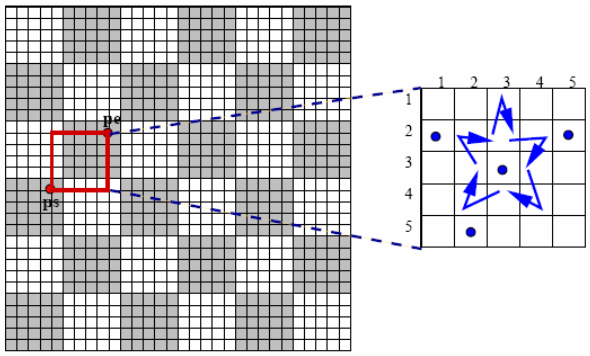

Figure 3 Grid Selection: Where User Selects A Drawing Grid For The Password [11]

2.2.4 Qualitative Draw -A-Secret

One possible limitation of graphical passwords is that they are more vulnerable to shoulder surfing than alphanumeric text passwords. This scheme is an extension and improvement on the Draw-a-Secret scheme originally proposed by [7] that is more resistant to shoulder surfing through the use of a qualitative mapping between user strokes and the password, and the use of dynamic grids to both obfuscate attributes of the user secret and encourage them to use different surface realizations of the secret. The use of qualitative spatial relations relaxes the tight constraints on the reconstruction of a secret; allowing a range of deviations from the original [12] .

Moreover, The QDAS drawing-grid is initially similar to a typical DAS grid however each cell in QDAS is explicitly annotated using an integer index. As for DAS, QDAS assumes stylus-based input and the user must create a sequence of strokes that they feel they can remember. Also different techniques of drawing selection must be developed as the proportions of any meaningful drawing are removed by grid transformations. Similar to DAS, there is a one-to-many relationship between an encoding and the corresponding free-form images. QDAS introduces two components that distinguish it from its DAS counterpart:

- qualitative spatial descriptions of strokes; meaning that encoding starts at 6, followed by “down”, “right”, and “up”.and
- the use of dynamic grid transformations as illustrated in figure 4.

The main aims of QDAS are as follows:

- to allow users to set strong secrets that do not impose load on long-term memory, and
- to be resistant to shoulder surfing.

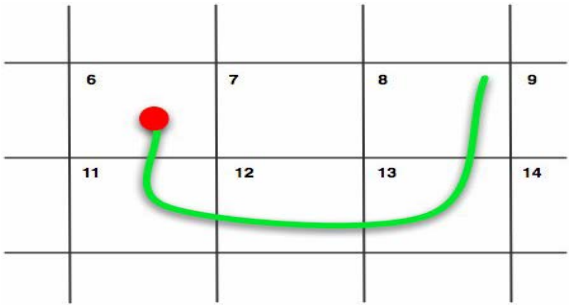

Figure 4. Qualitative Spatial Descriptions Of Strokes

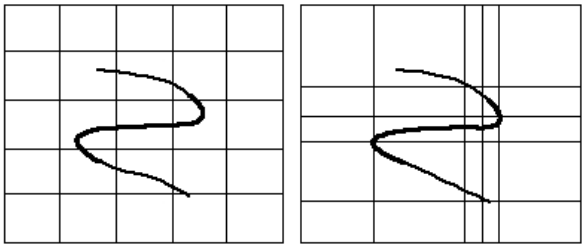

Figure 5: An Example Of The Dynamic Grids After A Stroke

2.2.5 Multi-Grid Graphical Password Scheme

Multi-grid is a knowledge-based graphical password technique and a good extension or alternative to the Draw-a-Secret scheme (DAS) proposed by Jermyn et al.[7] . In this scheme grid-squares not identical in size and shape as illustrated in figure 6 [13] and user draws a design on a display grid whose coordinates are used as the password. Multi-grid scheme of the DAS technique is inspired by the fact that users tend to draw lines and shapes on specific areas in the grid [13]. Therefore, the aim of this scheme is to decrease the password centering effect so that user could focus in a single internal grid, so there is more than one area where the password can be centered to. It was also claimed that the approach

Journal of Theoretical and Applied Information Technology
10th August 2013. Vol. 54 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

increases the password strength in user-friendly environment of the scheme.

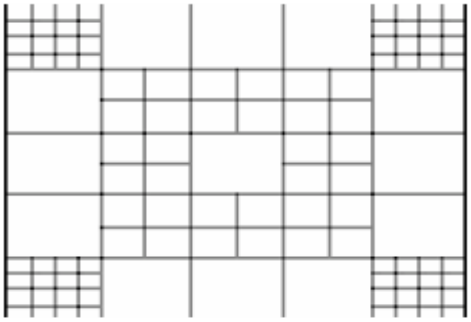

Figure 6: A Multi-Grid Template

2.2.6 Passdoodle Algorithm

Pass doodle (see figure 7) is another scheme similar to DAS except that it does not require use of visible grid. It is a graphical password scheme which was proposed in the year 2004 by Chistopher et al. The scheme was based on the idea of hand written designs or words, drawn with a pen onto a sensitive touchable screen without any visible grid as shown in figure 7 [14]. Doodle-based graphical passwords have been proposed as an alternative to traditional passwords in touch screen-enabled devices . Passdoodle loo In this system ,according to figure 7, users are validated by tracing a doodle over a touch screen, which is then accepted or rejected by the system. Due to their graphical nature, they are in general easier to remember than strings composed of characters and numbers. It only requires a touch screen, which is now popular in handheld devices, opposed to specific acquisition hardware needed to capture biometric traits such as fingerprints. Within biometrics, signature verification is the most similar trait with respect to doodles. Users are validated by tracing a doodle over a touch screen, which is then accepted or rejected by the system. Due to their graphical nature, they are in general easier to remember than strings composed of characters and numbers.

Figure 7: An Example Of A Passdoodle

2.2.6 Pass-Go

Pass-Go is a graphical password scheme, motivated by an old Chinese game, Go. The scheme was proposed by Hai Tao in 2006 as an improvement of the DAS which is the first grid based graphical algorithm [4]. For user to enter password in this scheme, he selects intersections instead of cells on a grid as illustrated in figure 8.

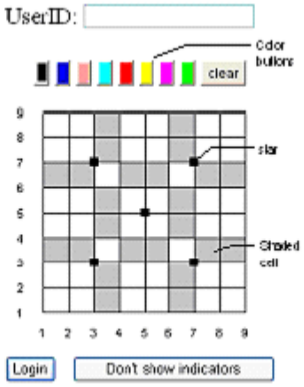

Figure 8: Pass-Go Scheme

By this difference of usage, the algorithm is referred to as a matrix of intersections, which is different from cell as in the case of DAS's scheme. The use of intersections as against cells allows the user to use password from greater password space (256 bits for the most basic scheme), and provides better usability than DAS counterpart. Also, the size of the grid in the Pass-Go changes to 9 * 9. Pass-Go scheme supports most application environments and input devices, rather than being limited to small mobile devices (PDAs), and can be used to derive cryptographic keys.

However, the limitations of the original scheme are as follows:

- Users suffer error tolerance mechanism because of the interceptions which are invisible areas usable by the user for password are difficult to know . In order , to solve this problem, the sensitive areas must be defined.
- The scheme is vulnerable to shoulder surfing attack.

Two versions of this scheme inspired by the above stated limitations are designed and implemented by Porn and his colleagues in order to enhance it . It was claimed to be better than

Journal of Theoretical and Applied Information Technology
10th August 2013. Vol. 54 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the original scheme in terms of usability and security.

2.2. 7 Haptic-based graphical scheme

Haptic-based graphical scheme was proposed by Malek et al. in year 2006 as another variation of draw-based scheme. The scheme was developed to protect against shoulder-surfing by making an observer to find it difficult to distinguish changes in pen pressure while drawing his or password. In this system, users make their passwords by drawing on a layout grid sometimes called passgrid . For illustration, see figure 8 where user draws password by starting from one point to another points, and finally to the original point , also with pressure on each point to deceive an on looker . This makes the scheme hard to break by an attacker as claimed by the author .However, the user study conducted revealed that small margin differences and that the use of haptics did not increase the difficulty of password guessing [3] because users applied just very little and hardly change the pen pressure while drawing their passwords. In their user study where 18 volunteers were made to use two different prototypes of 5x5 grids and 8x8 grids each. It was discovered by the users that it was easy to recall and repeat their passgrid with the smaller grid system while the larger grid system was more secure because of being larger in area [6] .

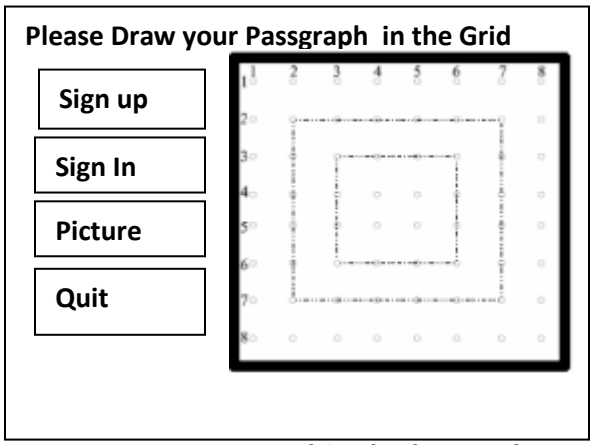

Figure 9: Haptic-Based Graphical Password

2.2.8 The GrIDsure graphical Scheme

GrIDsure is a commercial graphical scheme that uses 5x5 grid for accepting pattern during registration and displaying digits during authentication as illustrated in figure 9a&b . Registration grid displays bland cells of which four are used to register Personal Identification Pattern (PIP). During registration , users select and memorize a pattern over any four ordered cells in the grid of 25 cells. During the authentication stage, digits are randomly displayed on the grid then user enters only four digits appearing on the chosen pattern in the specific order with the help of keyboard without touching the grid. For the subsequent logins, users enter the new sequence of digits corresponding to the cells of their memorized pattern from randomly displayed digits over the grid cells [3]. The digits in the grid change randomly for every authentication because the system relies on One-Time Password or PIN (OTP) concept for its operation.

A	B	C	D	E
F	G	H	I	J
K	L	M	N	O
P	Q	R	S	T
U	V	W	X	Y

Figure 9: A) Registration Stage For Drawing User's Choice Pattern.

3	7	0	2	9
0	1	9	6	0
4	3	8	1	2
6	1	9	7	1
5	4	8	4	9
Enter Code:	*	*	*	*

Figure 9: B) Authentication Stage For Displaying Selecting Digits Corresponding To The Chosen Pattern Via The Keyboard.

2.2.9 YAGP: Yet Another Graphical Password Strategy

The enhanced YAGP is another extended version of DAS graphical scheme. It was originally developed by Gao et al. [15]. YAGP uses the strengths of DAS. YAGP scheme interface has a grid canvas with a granularity of 46x64 as illustrated in figure 10. The main difference between DAS and YAGP is soft matching which is used to describe the characteristics of the images rather than exact matching to help users from strict drawing rules and ultimately ease

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

usage. To provide these advantages, YAGP scheme introduces four (4) new concepts that were not found in DAS for better performance. The new concepts include ; Similarity by using Levenshtein Distance, trend quadrants to judge the tendency of each stroke, stroke-box and image-box which is required to depict the relative positions of strokes. This scheme is more usable than DAS and solves a number of DAS limitations for the users. Experiments were conducted to support the effectiveness of the scheme in terms of good memorabily and usability claims.

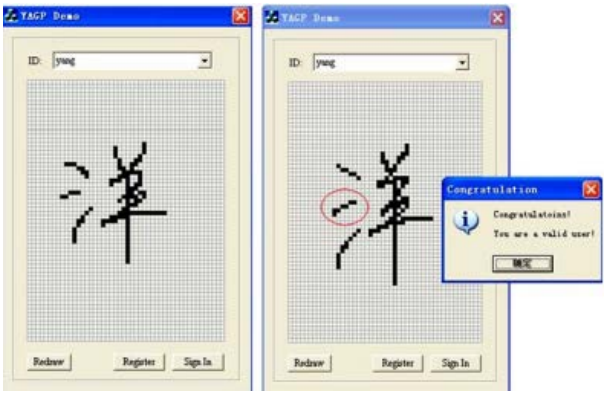

Figure 10:YAGP Scheme Interface Has A Grid Canvas With A Granularity Of 46x64

2.2.10 PassShape

The functions of this authentication system is based on the idea of use shapes as passwords instead of 4 digits for PIN or 8 alphanumeric characters for text-based systems. It involves 8 strokes directions that are set at 45^0 intervals based on observations of PIN or password entry methods. Unlike DAS, and PassGO schemes the drawing exact size is not necessary because passwords are encoded using strokes directions and not grid cells and interceptions respectively. In this system , a shape can be any of three kinds: horizontal, vertical and diagonal strokes. Figure 11 below, shows all eight possible strokes used in our approach.

[16]

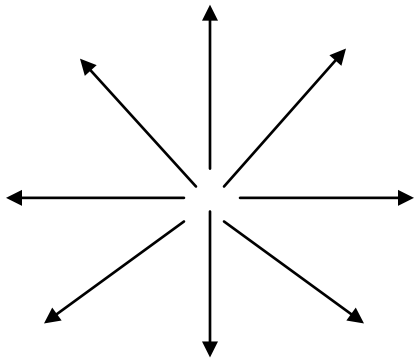

Figure 11:Shapepass Illustrating The 8 Possible Strokes

Table 3:Summary Of Studies On Draw-Based Password Schemes

Schemes	Studies
DAS[17]	Security aspect determines vulnerability to dictionary attacks on end users tendency to symmetric drawings. While the memorability studies provide login success rates.
BDAS[3]	Focused on how to improve the complexity of the passwords and to improve memorability in terms of better login rate.
Passdoodle [3]	Memorability test via login success rates.
Qualitative DAS[18]	Memorability studies on login success rates on a fewer of number of users.
Pass-Go [3]	On login success rate , login process, and even on security analysis to resist against shoulder-surfing attacks.
Grid Selection	Study on how to memorize and identify the correct grid cell used and to make sure users do not choose symmetric passwords.
Multi-Grid scheme	Memorability test via login success rates.
Haptic [19]	User studies to measure the effect haptic parameter on users and the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	net effect on guessing attack .
GrIDsure [3]	Memorability test on PDAs and login success rates.
YAGP[3]	Memorability test via login success rate and password complexity to resist against shoulder-surfing and brute-force attacks.
Pass Shape [16]	Memorability study test via login success rates and time.

3. Memorability of Draw-based Graphical Passwords

Passwords have ever been widely used as a means to confirm the identity of user in order to gain secure access to computers and communication systems. The problem of passwords is caused by the inability of user's memory to recall complex or random passwords which are secure without resorting to unethical practices such as writing down, using same password for multiple accounts, and using dictionary words. For this reason, graphical passwords are a better secure alternatives because they involve images and people have a amazing ability to recall images in long-term memory. Table 1 , illustrates the memorability of each scheme. Images depicts users' daily scenes and events even shapes of any forms that are appealing to users. The reason for this could be that some pictures contain usual things which are of interest to user, like friends, a fun involving family members, a particular moment during a trip or even strange images can be highly memorable[20] .

Phillip Isola and his team carried out a research study on how to systematically differentiate between images and knowing the intrinsic image features that make an image memorable [20] . Memory game was involved in their study where participants viewed a sequence of images that were used in the study to measure memorability of images. In the game, each image is displayed for 1 second for participant to view and commit to memory till (about 1.4 seconds) when he or she is expected to recognize same image at latter stage. This is illustrated in figure 11(a-c).The result of their study revealed that images memorability could be grouped into three categories[20] :

- Most memorable images -86% memorability.
- Typical images -74% memorability.
- Least memorable images -34% memorability.

Figure 11:Memory Game [20]

Figure 11a:Being One Of The Most Memorable Images (86%)[20]

Figure 11b:Being One Of The Typical Images (74%) [20]

Journal of Theoretical and Applied Information Technology
10th August 2013. Vol. 54 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 11c:Being One Of The Least Memorable Images (34%)[20]

Therefore, it is worthwhile to note that from the result of this research, the choice of background image for draw-based graphical passwords could affect their memorability. Therefore, choice of background image should be considered as a very important factor in the design of draw-based schemes with image background to achieve considerable memorability.

Table 1: Memorability Comparison Of Existing Draw-Based Graphical Schemes.

Schemes	**Recall Rate**	**Type of User Studies**	**Memorability feature**
Draw-A-Secret,DAS[17]	57-80%	Paper-based	Rectangular grid
BDAS[3]	50-80%	Paper proto-types	Graphical grid with background image
Passdoodle[3]	38-46%	Paper and Lab	Freehand design and comparison algorithms.
Qualitative DAS[18]	100%	Paper-based	Drawing of images in a predefined order.
Pass-Go [3]	78%	Long term field study.	Interception of lines in a grid instead of cells.
Grid Selection	-	-	Zoom feature (a smaller portion of graphical grid is required for the drawing)
Multi-Grid scheme	-	-	Grid-squares of different size and shape.
Haptic [19]	86.29 - 93.89 %	lab	Pen pressure technology using haptic input devices for detecting pressure
GrIDsure[3]	87% after 2 years	Long term lab studies	A Pattern connecting all the selected cells
YAGP[3]	87-96%	lab	Use of approximation algorithm
PassShape[16]	-	-	Shape and 8 strokes geometrical directions

4. CONCLUSION

Graphical passwords are generally and primarily made to address the usability and security limitations of text-based passwords which include memorable passwords are vulnerable to attacks while the random and long passwords are secure and not memorable. For random passwords to be useful , users employ coping practices which are not in agreement with laid down rules of password security. Draw-based graphical passwords was started with DAS that is able to provide passwords is clearly stronger than alphanumeric passwords but not extensively difficult to remember. Other modifications of DAS are surveyed in this study where in the course of study it was discovered that modified DASs are designed to solve DAS limitations in terms possible attacks against the DAS, centering effect and other usability challenges. However, memorability aspect of usability suffers

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

inadequate consideration. Meaning that more need to be done in this area for draw-based graphical passwords.

In this paper we have encouraged that considerable attention should be given to the choice of background image for schemes that require it to achieve better memorability. In future work, it will be worthwhile to investigate this claim in the design of graphical passwords by taking one image from each group for memorability test.

ACKNOWLEDGMENT

The authors would like to express their appreciation to Universiti Teknologi Malaysia , (UTM) for providing conducive environment for research. Also, the enormous support provided by the members of staff of Faculty of Computing is highly appreciated.

REFRENCES

[1]. 1. Gupta, S., et al., *Passblot: A Highly Scalable Graphical One Time Password System.* International Journal, 2012. **2**.
[2]. 2. Monrose, F. and M.K. Reiter, *Graphical passwords.* Security and Usability, 2005: p. 147-164.
[3]. 3. Biddle, R., S. Chiasson, and P.C. Van Oorschot, *Graphical passwords: Learning from the first twelve years.* ACM computing surveys (CSUR), 2012. **44**(4): p. 19.
[4]. 4. Tao, H., *Pass-Go, a new graphical password scheme*. 2006, University of Ottawa.
[5]. 5. Ray, P.P., *Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices.* Journal of Information Engineering and Applications, 2012. **2**(2): p. 1-11.
[6]. 6. Jali, M.Z., *A study of graphical alternatives for user authentication.* 2011.
[7]. 7. Jermyn, I., et al. *The design and analysis of graphical passwords*. 1999: Washington DC.
[8]. 8. Goldberg, J., J. Hagman, and V. Sazawal. *Doodling our way to better authentication.* 2002: ACM.
[9]. 9. Dunphy, P. and J. Yan. *Do background images improve Draw a Secret graphical passwords?* 2007: ACM.
[10]. 10. Thorpe, J. and P. Van Oorschot. *Towards secure design choices for implementing graphical passwords*. 2004: IEEE.
[11]. 11. Thorpe, J. and P. Van Oorschot. *Towards secure design choices for implementing graphical passwords.* in *Computer Security Applications Conference, 2004. 20th Annual*. 2004: IEEE.
[12]. 12. Lin, D., et al. *Graphical passwords & qualitative spatial relations.* 2007: ACM.
[13]. 13. Chalkias, K., A. Alexiadis, and G. Stephanides. *A multi-grid graphical password scheme*. 2006: Citeseer.
[14]. 14. Varenhorst, C., *Passdoodles: A lightweight authentication method.* Research Science Institute, 2004.
[15]. 15. Liu, X.-Y., et al., *An enhanced drawing reproduction graphical password strategy.* Journal of Computer Science and Technology, 2011. **26**(6): p. 988-999.
[16]. 16. De Luca, A., R. Weiss, and H. Hussmann. *PassShape: stroke based shape passwords.* in *Proceedings of the 19th Australasian Conference on Computer-Human interaction: Entertaining User interfaces*. 2007: ACM.
[17]. 17. Meng, Y. *Designing Click-Draw Based Graphical Password Scheme for Better Authentication*. in *Networking, Architecture and Storage (NAS), 2012 IEEE 7th International Conference on*. 2012: IEEE.
[18]. 18. Lin, D., et al. *Graphical passwords & qualitative spatial relations.* in *Proceedings of the 3rd symposium on Usable privacy and security*. 2007: ACM.
[19]. 19. Orozco, M., et al. *Haptic-based sensible graphical password*. in *Proceedings of Virtual Concept*. 2006: Citeseer.
[20]. 20. Isola, P., et al. *What makes an image memorable?* in *Computer Vision and Pattern Recognition (CVPR), 2011 IEEE Conference on*. 2011: IEEE.